SYSTEM AND METHOD FOR SECURE COMPARISON OF A COMMON SECRET OF COMMUNICATING DEVICES

ABSTRACT OF THE DISCLOSURE

A simplified authentication system for communicating devices having fewer security requirements than conventional cryptographic systems. The device to be authenticated includes a secret, a function component for generating a random number, a function component for exchanging messages with other devices and finally an algorithm for calculating a hash using random number and secret. The device requesting authentication includes a secret and an algorithm for calculating a hash using a random number received from the device to be authenticated. A function component for comparing both hashes may be implemented in both devices. If the hashes calculated by both devices match it can be assumed that the authentication was successful. Preferably, this system and method may be used within a communication structure using portable communication devices like smartcards, personal digital assistants or mobile phones. Neither an exchange of the plain secret itself nor the storage of digital keys is required. A misuse of the secret may be excluded by sending a hash using the random number and the secret. The infrastructure required by the present invention is very simple and does not consume storage capacity like conventional encryption methods, since digital keys and conventional symmetric or asymmetric algorithms are not required. Instead of using the digital keys and conventional symmetric or asymmetric algorithms, the present invention contemplates using a relatively simple random number and a simple hash algorithm, which sufficiently fulfills the security requirements of many communication architectures.